Quantum-Secured Space-Air-Ground Integrated Networks: Concept, Framework, and Case Study

Minrui Xu, Dusit Niyato, Zehui Xiong, Jiawen Kang, Xianbin Cao, Xuemin Sherman Shen, and Chunyan Miao

Abstract

In the upcoming 6G era, existing ground networks have evolved toward space-air-ground integrated networks (SAGIN), providing ultra-high data rates, seamless network coverage, and ubiquitous intelligence for communications of applications and services. However, conventional communications in SAGIN still face data confidentiality issues. Fortunately, the concept of Quantum Key Distribution (QKD) over SAGIN is able to provide information-theoretic security for secure communications in SAGIN with quantum cryptography. Therefore, in this article, we propose quantum-secured SAGIN (Q-SAGIN) which are feasible to achieve proven secure communications using quantum mechanics to protect data channels between space, aerial, and ground nodes. Moreover, we propose a universal QKD service provisioning framework to minimize the cost of QKD services under the uncertainty and dynamics of communications in Q-SAGIN. In this framework, fiber-based QKD services are deployed in passive optical networks with the advantages of low loss and high stability. Moreover, the widely covered and flexible satellite- and UAV-based QKD services are provisioned as a supplement during the real-time data transmission phase. Finally, to examine the effectiveness of the proposed concept and framework, a case study of Q-SAGIN in the Metaverse is conducted where uncertain and dynamic factors of the secure communications in Metaverse applications are effectively resolved in the proposed framework.

Introduction

The growing interest in the sixth generation (6G) wireless networks, particularly the comprehensive connectivity and trustworthiness offered by space-air-ground integrated networks (SAGIN) [1], is pushing the current communication infrastructure to its limits. However, secure communications of SAGIN are under serious threats in the post-quantum era. Currently, symmetric-key cryptography and public-key cryptography are used to protect the confidentiality of sensitive data in SAGIN, which are no longer considered safe with the advent of quantum computers [2]. On the one hand, quantum computers can address some large-scale NP-hard mixed integer resource allocation problems in SAGIN [3]. On the other hand, the integer factorization and discrete logarithm problems can be easily compromised by a quantum computer that is advanced in computational power and quantum algorithms (e.g., Shor's algorithm). Fortunately, data channels of SAGIN can be secured by quantum cryptography, which uses quantum key distribution (QKD) to provision secret cryptographic keys via quantum channels and key management (KM) channels [4]. In the post-quantum era, communications in quantum-secured SAGIN (Q-SAGIN) are expected to achieve the information-theoretic security with the guarantees of the principles of quantum physics, as guaranteed by the quantum no-cloning theorem and the Heisenberg's uncertainty principle [5].

In Q-SAGIN, the concept of QKD over SAGIN typically allows two remote QKD nodes to exchange quantum bits (qubits) which encode classical bits on quantum states, such as photons, through optical fibers or free sptace [5]. As shown in Fig. 1, the optical fiber-based QKD is a mature option based on the wavelength-division multiplexing (WDM) technique to transmit qubits and bits in the same fiber with a low loss and high stability. However, since qubits are more vulnerable to propagation impairments and cannot be readily amplified, the optical fiber-based QKD has limited distance requirements as its secret-key rate decreases exponentially when the distance increases. Therefore, as an alternative option, QKD via free space [6–8], for example, satellite-based QKD and unmanned aerial vehicle (UAV)-based QKD, is more effective to transmit qubits with advantages of wide coverage and high flexibility. As a result, the concept of QKD over SAGIN, which comprises optical fiber-based QKD from the ground subnetwork, satellite-based QKD from the space subnetwork, and UAV-based QKD from the aerial subnetwork, provides a feasible solution for Q-SAGIN.

Although Q-SAGIN are feasible through the concept of QKD over SAGIN, an efficient service provisioning framework is still necessary to manage and control QKD resources for optimizing the provisioning cost. To this end, a universal framework is proposed to offer secret-key distribution services to QKD nodes with security requests, that is, secure communication requests, which may contain different secret-key sizes, rates, and updating periods [5]. By optimizing the deployment of

Minrui Xu, Dusit Niyato, and Chunyan Miao are with Nanyang Technological University, Singapore; Zehui Xiong (corresponding author) is with Singapore University of Technology and Design, Singapore; Jiawen Kang is with Guangdong University of Technology, China; Xianbin Cao is with Beihang University, China Xuemin Sherman Shen is with the University of Waterloo, Canada.

Digital Object Identifier:
10.1109/MWC.008.2200163

1536-1284/23/$25.00 © 2023 IEEE

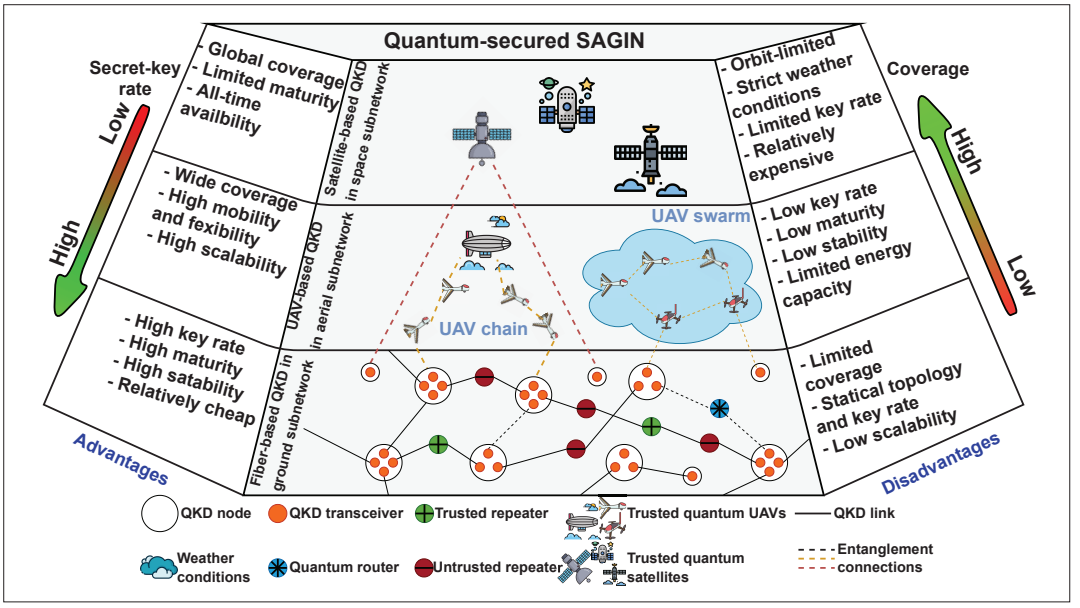

FIGURE 1. The concept of QKD over SAGIN in quantum-secured SAGIN.

QKD resources, such as QKD nodes and links, the framework can cost-effectively provision QKD services. In detail, the framework provides optical fiber-based QKD services statically with a fixed and relatively low cost. However, only the stationary QKD services may not be sufficient to secure the transmission of confidential data in dynamic communication environments. Therefore, the uncertainty in secure communication environments necessitates the provisioning of satellite- and UAV-based QKD services, according to the real-time secure communication requests flexibly with high cost. To verify the effectiveness of the aforementioned concept and framework, the Metaverse [9] is used as a use case where Metaverse users and applications transmit data via Q-SAGIN. The data generated and transmitted by the Metaverse applications, such as extended reality (XR), digital twin, and artificial intelligence (AI), is often communication-heavy, high-frequent, and asynchronous. For example, Metaverse users receive immersive experiences with their avatars in the 3D worlds of the Metaverse through XR, including augmented reality (AR), virtual reality (VR), and mixed reality (MR). Since each user can control multiple avatars in the Metaverse simultaneously, the number of avatars in the Metaverse cannot be accurately predicted by the QKD service provisioning framework. Second, due to the continuously varying importance of the real-world environment, the transmission speed and update frequency of the digital twins in the Metaverse also fluctuate. Third, the number of AI models in the Metaverse also varies depending on the amount of AI data and computational power (e.g., the number of workers in federated learning [4]). Based on the stochastic programming of QKD services, the proposed universal framework is expected to resolve the uncertainty issues in security requests and to minimize the provisioning cost. The experimental results demonstrate that although providing QKD services for Metaverse applications in Q-SAGIN is an intricate problem, the proposed stochastic programming model can still optimize the required cost of QKD service provisioning.

Our main contributions can be summarized as follows:

- We highlight the feasibility of Q-SAGIN through the concept of QKD that we present. To the best of our knowledge, this is the first work to propose Q-SAGIN where the QKD services can holistically secure communications between space, aerial, and ground nodes using quantum cryptography.
- We propose a universal service provisioning framework to realize the concept of QKD over SAGIN. With uncertain communications and security requirements in Q-SAGIN being taken into account, the proposed framework can provide flexible QKD services while minimizing the provisioning cost in Q-SAGIN.
- As a case study, we examine the effectiveness of Q-SAGIN and its service provisioning framework in supporting Metaverse applications. By considering the uncertain factors in the communications of Metaverse applications, the proposed framework can achieve an optimal provisioning solution for QKD services. The experimental results show that the proposed framework outperforms the existing baseline methods while addressing the uncertainty of communication environments with the varying number of avatars, digital twins, and AI models.

The Concept of QKD over SAGIN and the Quantum-Secured SAGIN

The Basic Concept of QKD

QKD has recently been introduced as a provable secure key distribution solution that can address many potential attacks, such as eavesdropping attacks, in traditional key distribution schemes [10]. In practice, QKD is often adopted in the setup phase of secure communications between two nodes connected with QKD logical links for transmitting confidential data. During the setup of secure communications between two QKD nodes, they first need to agree on a global secret cryptographic key (i.e., a sequence of bits) via

QKD types	Transmission media	QKD protocols	QKD resources	Distance (km)
Optical fiber-based QKD	Optical fibers	Prepare-and-measure/Entanglement-based QKD protocols	Quantum transceivers, trusted/untrusted repeaters, quantum routers, quantum memory, QKD links	~ 100
Satellite-based QKD	Free space	Entanglement-based QKD protocols	Trusted quantum satellites, quantum memory, QKD links	~ 1000
UAV-based QKD	Free space	Entanglement-based QKD protocols	Trusted quantum UAVs, quantum memory, mobile QKD links	~ 1

TABLE 1. Summary of different QKD services in Quantum-secured SAGIN.

QKD links, where any eavesdropping or hijacking behaviors during key agreement process can be perceived due to the quantum no-cloning theorem [2]. Therefore, in QKD logical links, their raw local secret keys are encoded as certain quantum states of photons and transmitted in quantum channels while the exchanged classical key information is verified and processed in KM channels.

QKD over SAGIN

Optical Fiber-Based QKD Services: Existing conventional passive optical networks (PON) provide the maturest and cheapest implementation scenario for fiber-based QKD in the ground subnetwork. With the WDM technique, qubits and bits can be transmitted together in the same optical fiber with low loss and high stability. As the optical fiber-based QKD is established upon the existing PON, its components are co-located with the backbone nodes in PON. There are three types of QKD nodes in optical-based QKD, that is, quantum transmitters/receivers (transceivers, TCs), trusted/untrusted repeaters, and quantum routers. Firstly, each TC is a pair of QKD equipment, including a quantum transmitter and a quantum receiver, that can convert bits of local secret keys into qubits and convert qubits into bits of global secret keys, respectively, via prepare-and-measure protocols, for example, Bennett-Brassard-1984 (BB84), Grosshans-Grangier-2002 (GG02) [10]. Then, the received secure keys are saved by their respective local key managers. Extending from the above point-to-point scenario, optical fiber-based QKD with trusted repeaters can distribute secret keys in a hop-by-hop manner to improve the key distribution distance. Furthermore, in the measurement-device-independent (MDI)-QKD protocol [11], untrusted repeaters typically have better security than other prepare-and-measure protocols requiring only trusted repeaters, which can remove the security infrastructure at the measurement side. Therefore, the untrusted repeater can even be controlled by an eavesdropper without compromising the safety of QKD. Therefore, MDI-QKD protocols are capable of improving the secure distance and efficiency of QKD considerably. Different from prepare-and-measure protocols, entanglement-based protocols, such as Bennett-Brassard-Mermin-1992 (BBM92) [7], implement quantum routers with quantum memory to distribute secret keys via quantum entanglement of photons over different quantum channels. Between two adjacent quantum routers, each external link is established where one of the qubits in a Bell pair should be sent to the other quantum router of this external link, and hence one unit of quantum memory on each router needs to be occupied [12]. Then, quantum routers perform entanglement swapping to measure the qubits and route the result to the destination router via the internal link of an entanglement connection. For the optical fiber-based QKD services in the ground subnetwork, TCs and QKD links of trusted/untrusted repeaters as well as quantum memory of quantum routers are collectively regarded as QKD resources in provisioning QKD services over SAGIN. However, the fixed topology of PON limits the secret-key rate and scalability of optical fiber-based services. Moreover, field experiments on free-space QKD transmission in the ground subnetwork are still pending [10].

Satellite-Based QKD Services: **Different from t**he optical fiber-based QKD with limited coverage in the ground subnetwork, the satellite-based QKD in the space subnetwork can provision QKD services with global coverage to ground QKD nodes from low earth orbit (LEO) satellites via free space [13]. Due to scattering and absorption of polarized photons and other factors, the requirements of trusted/untrusted repeaters to extend the coverage of optical fiber-based QKD place an obstacle to developing metropolitan-level QKD networks. Fortunately, satellite-based QKD in the space subnetwork is a promising scheme to distribute secret keys to ground QKD nodes via free space with less atmospheric attenuation. China sent its first quantum satellite, called Micius, into space in 2016 and completed an experimental satellite-to-ground QKD in good weather and night conditions. In June 2020, Micius experimentally demonstrated that satellite-based QKD could achieve a secret-key rate of 0.12 bits per second between two ground QKD nodes separated by 1120 km [7]. In satellite-based QKD, satellites are trusted quantum relays with all-time availability to establish entanglement connections between a pair of ground QKD nodes with polarization beam splitters. However, the deployment of satellite-based QKD services is relatively expensive and has limited maturity.

UAV-Based QKD Services: LEO satellites are orbit-limited and weather-constrained that cannot satisfy all the security requests on trusted UAVs carrying quantum equipment. Therefore, satellite-based QKD services can provide a wide coverage solution to serve ground QKD nodes regardless of the weather conditions. By transmitting quantum information as "flying quantum bits," UAVs in the aerial subnetwork can secure communications in SAGIN with a high degree of mobility and flexibility [13]. Specifically, two UAVs can achieve mobile entanglement distribution via free-space quantum channels and KM channels, with one distributing entangled photons and the

other acting as a relay node. However, beam-diffraction, which depends on the beam aperture and the link distance, limits the distance of the UAV-based QKD via free space. To address these issues, multiple UAVs can form swarms or chains, to distribute the quantum entanglement collaboratively for lossless propagation within the Rayleigh length limit. The experimental results in [8] show that UAV-based QKD can achieve high-performance quantum entanglement between two ground QKD nodes with polarization beam splitters at a distance of about 1 km. Due to the inexpensive and flexible nature of UAV swarms and chains, UAV-based QKD can provide high scalable QKD services in an economical manner. However, the low secret-key rate offered by single UAV swarms and chains and the limited energy capacity of UAVs still need to be addressed before the practical deployment of current immature UAV-based QKD services.

Establishing Secure Communications in Quantum-Secured SAGIN

In Q-SAGIN, a pair of two QKD nodes can establish secure communications via QKD links for transmitting confidential data. As shown in Table 1, If QKD nodes are directly or indirectly connected via optical fibers, they can continuously receive secret keys from optical fiber-based QKD services. Otherwise, QKD nodes can require the QKD services via free space from quantum satellites or quantum UAVs. On the one hand, satellite-based QKD services can distribute quantum entanglement in global coverage but are limited by the orbits of satellites and the weather conditions of ground nodes. On the other hand, UAV-based QKD can provision reconfigurable QKD services regardless of the location and weather condition of ground nodes. Through the concept of QKD over SAGIN, Q-SAGIN is feasible with unparalleled mobility, flexibility, and reconfigured by provisioning the QKD services via optical fibers, satellites, and UAVs synergistically.

The Universal QKD Service Provisioning Framework in Quantum-Secured SAGIN

Provisioning Static QKD Services via Optical Fiber-Based QKD

In the ground subnetwork of Q-SAGIN, optical fiber-based QKD is able to provision static QKD services by allocating QKD resources in terms of QKD nodes, for example, quantum transceivers, trusted/untrusted repeaters, quantum routers, and QKD links, as shown in Fig. 2. In Q-SAGIN, cryptographic applications initiate requests for QKD services to the QKD global manager, a centralized server in Q-SAGIN. Upon receiving these QKD service requests, the QKD global manager sends instructions to the optical fiber-based QKD controller via the simple network management protocol (SNMP). The management signals are encoded as qubits and transmitted in QKD links so that the data transmission is also quantum-secured. If the secret keys in the local key managers of the requesting QKD nodes are sufficient to satisfy these requests, the optical fiber-based QKD controller configures the QKD nodes and lets them provide the secret key to the cryptographic applications. However, since the coverage of optical fiber-based QKD services is limited and fixed, the optical fiber-based QKD services are not able to provide sufficient secret keys to well handle the uncertainty and dynamics in secure communications of QKD nodes.

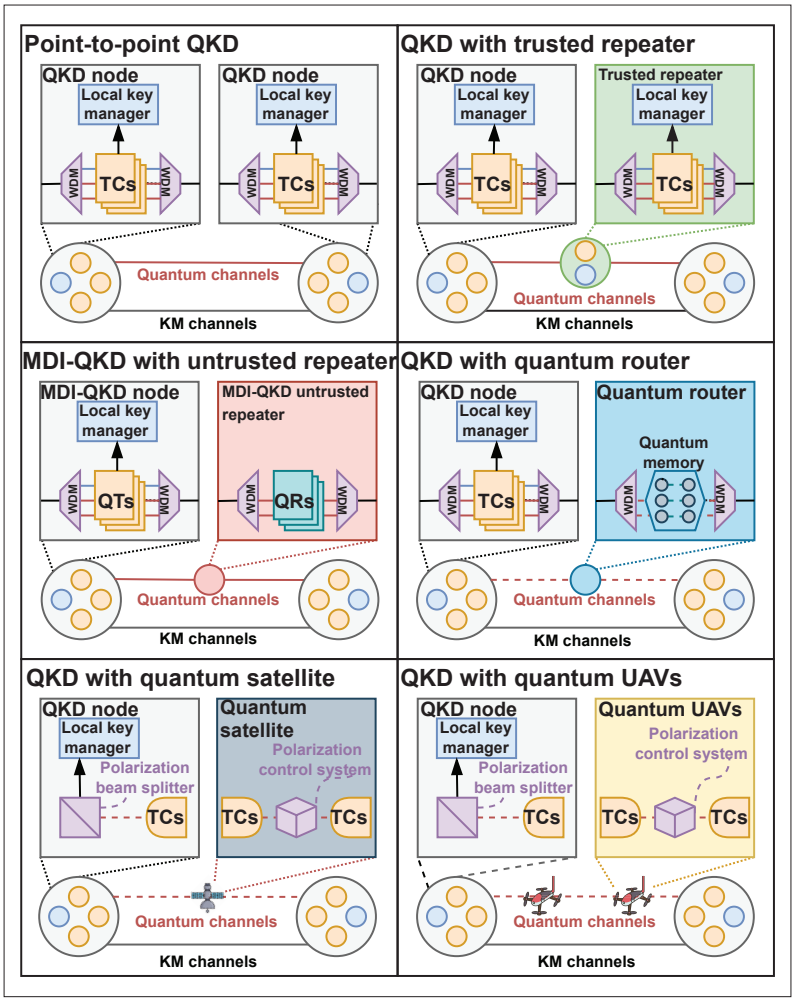

FIGURE 2. Different types of QKD resources in quantum-secured SAGIN. QTs, MDI-QKD transmitters; QRs, MDI-QKD receivers.

Provisioning Dynamic QKD Services via Satellite- and UAV-Based QKD

Fortunately, satellite- and UAV-based QKD services can supplement the required secret keys for QKD nodes to resolve the uncertain security requests in their communications with high coverage and flexibility. On the one hand, when the secret keys are not enough in the ground subnetwork, the satellite-based QKD controller can configure LEO satellites to distribute the required QKD services via satellite-based QKD in the space subnetwork. Although satellite-based QKD services are real-time and have global coverage, they are orbit-limited and constrained by the weather conditions of the ground nodes. Therefore, on the other hand, UAV-based QKD in the aerial subnetwork may be a practical alternative to provision QKD services at various times, locations, and weather conditions. According to the instructions from the QKD global manager during the data transmission phase, the UAV-based QKD controller can deploy UAV swarms or chains to provide QKD services in mobile quantum networks [13].

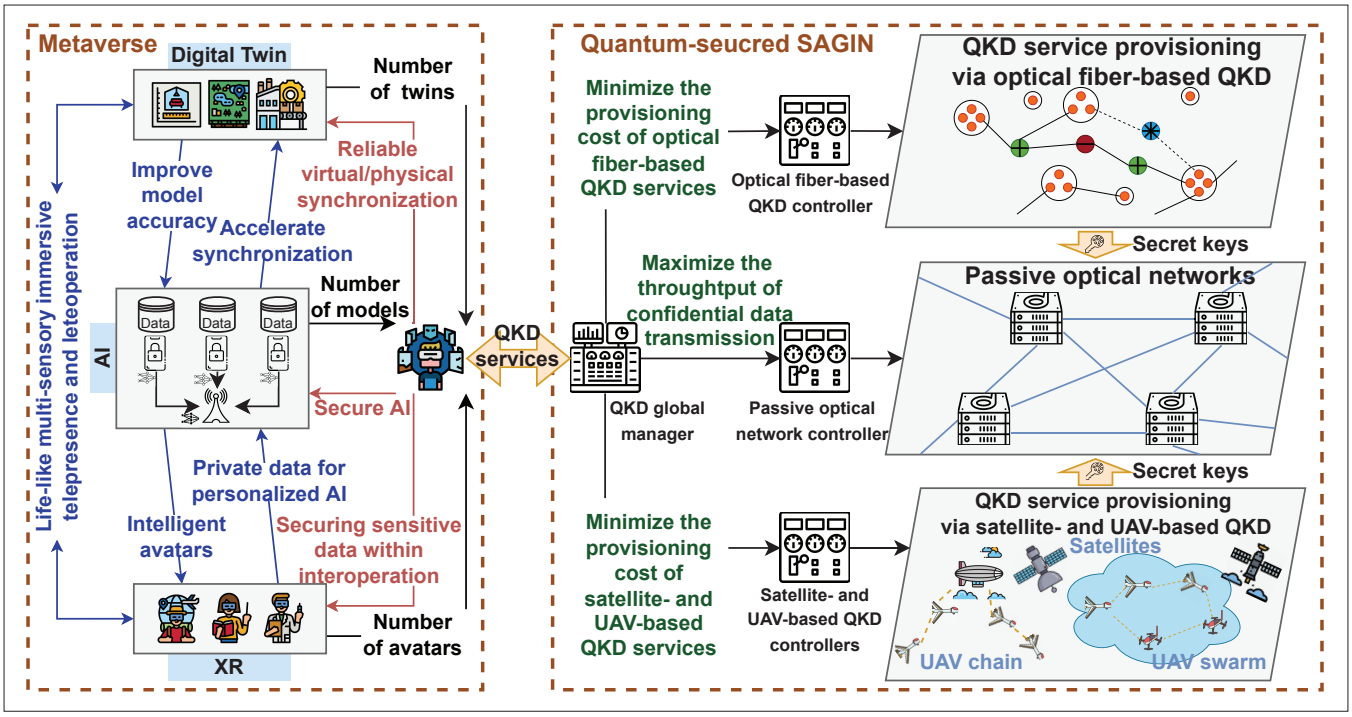

FIGURE 3. The universal QKD service provisioning framework with two-stage stochastic programming for Metaverse applications in quantum-secured SAGIN.

Challenges of Provisioning QKD Services in Quantum-Secured SAGIN

Efficient Routing for QKD Services: To provide efficient QKD services in Q-SAGIN, many practical challenges are required to be solved. First and foremost is the problem of point-to-point routing in optical fiber-based QKD in the ground subnetwork. Unlike routing in traditional backbone networks, optical fiber-based QKD requires nodes on the path of secure communications to be fully active and have enough secret keys. As shown in Fig. 1, there are two relaying nodes for the current optical fiber-based QKD, that is, trusted/untrusted repeaters and quantum routers. In optical fiber-based QKD services with trusted/untrusted repeaters, the nodes are connected with the intermediate of trusted/untrusted repeaters and the secret keys as well as key management information through QKD links and the encrypted message are transmitted through public data channels. Unlike the store-and-forward mechanism of trusted repeaters, the motivation of the implementation of quantum routers is to apply the quantum entanglement of photons to transmit quantum signals over different quantum channels. In other words, multiple quantum memory are connected together and the measurement of one of the quantum memory can change the quantum states of the other quantum memory. Even when a considerable distance separates the photons, they still establish a joint quantum system. For optical fiber-based QKD services, each distribution of the secret key information consumes a certain amount of quantum resources of QKD nodes. Since the quantum resources in each node are limited, the secret keys of each QKD node are also limited. The purpose of efficient routing for QKD services is to minimize the secret key consumption, that is, the number of hops transmitted, while satisfying the secure communication requests [14].

Uncertainty and Dynamics of Secure Communication Environments in Q-SAGIN: Q-SAGIN still need an effective dynamic resource management scheme to enhance the efficiency in provisioning QKD services. The communication security in Q-SAGIN is guaranteed by secret keys. The encryption operation of QKD nodes cannot be implemented without the secret keys in their local key managers, and thus the encrypted communication link is temporarily invalid. Although one-time pad encryption can provide information-theoretically secure (ITS) communication, due to the limited secret key provided by optical fiber-based QKD services, the requirement for the one-time pad to have an encryption key of equal length to the plaintext is difficult to achieve [10]. Therefore, the current solution of Q-SAGIN generally updates the secret keys periodically to ensure a certain level of secure communications. Nevertheless, before the transmission of confidential data, the data rate is unpredictable and QKD services provisioned by optical fiber-QKD are fixed and undersubscribed. Therefore, allocating satellite- and UAV-based QKD services to compensate for the secret key shortage is challenging to resolve the uncertainty and dynamics of secure communication environments.

Case Study: Metaverse in Quantum-Secured SAGIN

As illustrated in Fig. 3, in this case study of Metaverse in Q-SAGIN, we first provide an overview of Metaverse and highlight the requirements for secure interoperations of Metaverse applications. To provide QKD services for Metaverse applications, we develop the system model, provisioning options, and serving phases for QKD

over SAGIN. Finally, we describe the uncertainty of Metaverse applications and propose an optimization solution to provide QKD services cost-effectively.

Metaverse Applications

The Metaverse, considered as the successor to the mobile Internet, is a set of interoperable 3D worlds where people can telepresent themselves to work, play, and socialize [9]. In the Metaverse, applications/users provide seamless interoperations with other applications/users by constantly communicating with each other. As shown in Fig. 3, interoperations between XR and digital twin are required to provide life-like, multi-sensory, immersive telepresence and teleoperation between users and the real world. AI can be used to accelerate physical/virtual synchronization in the digital twin, and AI can then use the sensory data to improve the accuracy of AI models. In addition, Metaverse users enter the Metaverse in the form of avatars and interact with the Metaverse's intelligent avatars while using their private data to create personalized AI models. However, the embodied experiences provided by Metaverse applications make Metaverse users more vulnerable to threats of unsafe interoperability, such as unreliable virtual/physical synchronization, untrustworthy AI training and inference, and sensitive data leakage. Especially, in the post-quantum era, quantum computing is believed to be the cornerstone of the Metaverse applications and can be used for XR rendering, digital twin scientific calculations, and AI model training. However, quantum computing can compromise the secure interoperations of Metaverse applications based on traditional symmetric-key cryptography and public-key cryptography. Fortunately, QKD can provide information-theoretically secure interoperations for Metaverse applications. Moreover, QKD over SAGIN can secure the interoperations of Metaverse applications in a timely and global manner via Q-SAGIN.

System Model, Provisioning Options, and Serving Phases

To provision the QKD services to Metaverse applications, the system model of Q-SAGIN includes data nodes, QKD nodes and edges [15]. Here, data nodes are co-located with the QKD nodes. Edges in Q-SAGIN are QKD links, for example, optical fibers and entanglement connections, depending on the equipment of QKD nodes. For optical fiber-based QKD, each QKD node consists of a local key manager, and one or more transceivers of MDI-QKD. Between a pair of QKD nodes linked with optical fiber, a QKD link with multiple trusted/untrusted repeaters can be deployed for global secret key generation. Each trusted repeater consists of two or more QKD transceivers, a local key manager, and security infrastructure, while each untrusted repeater consists of two or more QKD transceivers but with a higher security level. For satellite- and UAV-based QKD, trusted quantum satellites and trusted quantum UAVs act as quantum relays.

The QKD global manager can offer secure communications of Metaverse applications in Q-SAGIN with two provisioning options, that is, QKD via optical fiber and QKD via free space. In general, the option of QKD via optical fiber provides QKD services through optical fiber-based QKD, while the option of QKD via free space provides QKD-supported secure communication services through satellite- and UAV-based QKD. However, the QKD via free space is more dynamic and its use can be on a short-term on-demand basis. It is important to note here that these provisioning options are similar to that of other network and cloud services available commercially, that is, reservation and on-demand subscription plans.

QKD service provisioning in Q-SAGIN is divided into three serving phases by the QKD global manager, that is, QKD via optical fibers, data transmission, and QKD via free space. First, in the phase of optical fiber-based QKD phase, the QKD global manager follows the option of QKD via optical fiber to instruct the optical fiber-based QKD controller to deploy optical fiber-based QKD services. As this should be done on a long-term basis, this option could be done without knowing the secure communication requirements of Metaverse applications. Then, when the option of QKD via optical fiber is determined, Q-SAGIN enters the data transmission phase. As the QKD via optical fiber is more stable and can be done on a long-term reservation basis, the secret keys provided by optical fiber-based QKD services are static. During the data transmission phase, if the security requirements of Metaverse applications incurs more secret keys which cannot be provided only by optical fiber-based QKD services, the Metaverse applications can request additional QKD services from the QKD global manager in the option of QKD via free space and then obtain more secret-key rate from the QKD via free space option. In this phase, the QKD global manager sends instructions to the satellite- and UAV-based QKD controllers to configure QKD services for Metaverse applications requiring extra QKD services. For the same secret-key rate, the provisioning cost of QKD via optical fibers is typically less than that of QKD via free space, for example, due to the network operating costs. The QKD global manager aims to satisfy the security requests of Metaverse applications while minimizing the provisioning cost of QKD services.

Uncertainty of Metaverse Applications in Quantum-Secured SAGIN

Under uncertainty of secure interoperations of Metaverse applications, the secret key rate of required QKD services by Metaverse applications is not precisely known when the option of QKD via optical fibers is made. Moreover, since the data transmission rates in the Metaverse fluctuate over time, the Metaverse applications cannot predict the required QKD services precisely. For example, due to the fact that AI data quantity and quality generated in Metaverse applications are varying over time, the frequency and size of updates to AI models are uncertain. Second, the number of digital twins is unpredictable and the synchronizing sizes and frequencies are varying according to the changing importance of the real-world environment. Third, the number of avatars in the Metaverse is dynamic, as each user can have multiple avatars simultaneously in different virtual 3D worlds. In general, the probability distribution of uncertainty can be partially fitted by statistical processes and machine learning.

In the Metaverse, applications/users provide seamless interoperations with other applications/users by constantly communicating with each other.

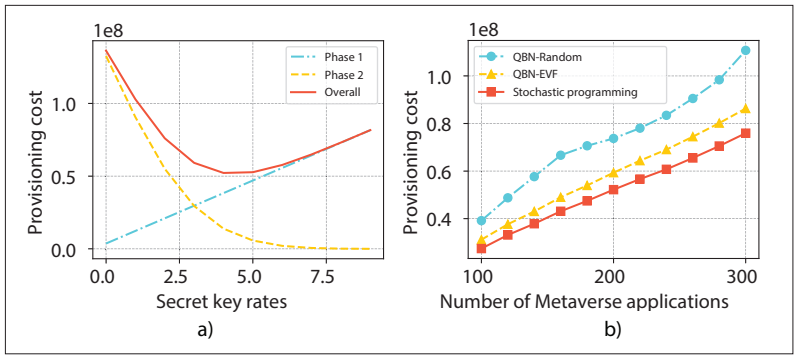

FIGURE 4. The cost structure and performance comparison of stochastic programming for secure communications of Metaverse applications in Q-SAGIN.

The Proposed Optimization Solution Approach

In the deterministic programming model for QKD service provisioning in Q-SAGIN, the required secret keys in QKD services of Metaverse applications are assumed to be exactly known by the QKD global manager. However, due to the aforementioned challenges in the QKD service provisioning framework and uncertain factors of secure communication environments in Metaverse applications, the QKD service requests for secure communications cannot be predicted precisely and fulfilled perfectly. Thus, the stochastic programming with two-stage QKD service provisioning is proposed. The first stage defined the number of optical fiber-based QKD services provisioned in the ground subnetwork, while the second stage defines the number of satellite- and UAV-based QKD services deployed in the space subnetwork and the aerial subnetwork. The stochastic programming model can be formulated as the minimization of provisioning cost including two parts, where the first part is the provisioning cost of optical fiber-based QKD services according to the option of QKD via optical fibers and the second part is the expected provisioning cost of the option of QKD via free space under the set of possible realized data transmission requests of Metaverse applications. The constraints of the stochastic programming model for QKD over SAGIN are flow conservation, the required number of wavelengths, transmission path uniqueness, wavelength continuity, wavelength capacity, and wavelength uniqueness [15] under the uncertainty of secure communication environments in Metaverse applications.

Experimental Results

The experiments are performed on the USNET topology with 24 nodes [10]. The distance between each pair of QKD nodes in optical fiber-based QKD is set to 80 km and the distance between each pair of UAVs in UAV-based QKD is set to 1 km. The required secret keys of Metaverse applications are set to the equivalent level. To simplify the evaluation, the uncertainty is reformulated as all the Metaverse applications have the equivalent requested size of secret keys that is determined by the amount of scenarios. For each scenario, the probability distribution of secret keys requirements follows a Poisson process with an average of the number of scenarios (set to ten) divided by three. Unless otherwise stated, the number of Metaverse applications is set to 200, including 20 security requests from avatars, 80 security requests from digital twins, and 100 security requests from AI models. Finally, the reservation cost values, with a unit denoting a unit of normalized monetary, of QKD transmitters, QKD receivers, local key manager, security infrastructure, MUX/DEMUX components, and optical fiber, are 1500, 2250, 1200, 150, 300, and 1, respectively. The on-demand cost values, with a unit representing a normalized monetary unit, of QKD transmitters, QKD receivers, secure-key buffers, security infrastructure, UAVs, and satellites are 6000, 9000, 3000, 500, 20, and 20000, respectively. QKD devices are relatively expensive, however, a small secret key can accomplish the encryption of a large amount of confidential data for example, a 256-bit secret key can be used to encrypt 64 GiB data in AES-256-GSM. Furthermore, new quantum infrastructures are required to be deployed for QKD service provisioning which will be the fundamental deployment of the upcoming quantum Internet [2].

Based on the aforementioned experimental settings, the cost structure of stochastic programming of QKD services in Q-SAGIN is first studied. As illustrated in Fig. 4a, the first stage, the second stage, and the overall provisioning costs vary as the number of reserved QKD services increases. As expected, the first stage provisioning cost linearly increases as the number of reserved QKD services rises. Nevertheless, during the data transmission, the second stage cost decreases as the number of reserved QKD services increases, so that less on-demand compensation is required for Metaverse applications. In this way, the optimized provisioning plan can be determined by the minimization of overall cost, for example, when the size of secret keys provided by optical-based QKD services equals to four as illustrated in Fig. 4a. Through cost analysis in QKD service provisioning framework, the optimal provisioning plan can not easily be obtained due to the uncertainty in the secure interoperations of Metaverse applications. For example, the optimal QKD service provisioning solution is not the place where the cost curves of the two stages of service are intersected. Therefore, a stochastic programming model for QKD over SAGIN is essential to achieve the minimized service provisioning cost.

In the experiments, two baseline algorithms, that is, the quantum backbone network (QBN) model with expected value formulation (QBN-EVF) provisioning and the QBN with random (QBN-Random) provisioning, developed in [10], are used for the compassion of the stochastic programming model. The provisioning costs of QBN-Random, QBN-EVF, and stochastic programming for different number of security requests in Metaverse applications are shown in Fig. 4b. We can observe that as the number of Metaverse applications increases, the provisioning costs of all three models increase accordingly. Moreover, the performance difference in provisioning cost among the three models is also larger as the number of Metaverse applications increases. In particular, the provisioning cost of QBN-EVF is slightly higher than that of the stochastic programming model, while the provisioning cost of QBN-Random is 50 percent higher.

Conclusion

In this article, we have highlighted the feasibility of Q-SAGIN through the conceptualization of QKD over SAGIN. We have presented the concept of QKD over SAGIN, where optical fiber-based QKD, satellite-based QKD, and UAV-based QKD services are provisioned collaboratively to secure communications in SAGIN. To realize the concept of QKD over SAGIN, we have proposed a universal QKD service provisioning framework which is expected to cater flexible and cost-efficient QKD services in Q-SAGIN. Finally, we have examined the proposed concept and framework by using Metaverse applications as a case study. The experimental results have demonstrated that proposed methods can minimize the provisioning cost under uncertain secure communication environments.

Acknowledgments

This research is supported in part by the National Research Foundation (NRF) and Infocomm Media Development Authority under the Future Communications Research & Development Programme (FCP) (FCP-NTU-RG-2021-014), under the AI Singapore Programme (AISG) (AISG2-RP-2020-019), under Energy Research Test-Bed and Industry Partnership Funding Initiative, part of the Energy Grid (EG) 2.0 programme, under DesCartes and the Campus for Research Excellence and Technological Enterprise (CREATE) programme, Alibaba Group through Alibaba Innovative Research (AIR) Program and Alibaba-NTU Singapore Joint Research Institute (JRI), Singapore Ministry of Education (MOE) Tier 1 (RG16/20), the SUTD SRG-ISTD-2021-165, the SUTD-ZJU IDEA Grant (SUTD-ZJU (VP) 202102), the SUTD-ZJU IDEA Seed Grant (SUTD-ZJU (SD) 202101), and NSFC under grant No. 62102099, Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (No. ICT2022B12).

References

[1] H. Cui *et al.*, "Space-Air-Ground Integrated Network (Sagin) for 6g: Requirements, Architecture and Challenges," *China Commun.*, vol. 19, no. 2, 2022, pp. 90–108.
[2] C. Wang *et al.*, "Application Scenarios for the Quantum Internet," Internet-Draft draft-irtf-qirgquantum- internet-use-cases-10, Internet Engineering Task Force, Mar. 2022. Work in Progress.
[3] Z. Zhao, L. Fan, and Z. Han, "Hybrid Quantum Benders' Decomposition for Mixed-Integer Linear Programming," *Proc. 2022 IEEE Wireless Commun. and Networking Conf.*, IEEE, 2022, pp. 2536–40.
[4] A. Huang *et al.*, "Starfl: Hybrid Federated Learning Architecture for Smart Urban Computing," *ACM Trans. Intelligent Systems and Technology*, vol. 12, no. 4, 2021, pp. 1–23.
[5] M. Mehic *et al.*, "Quantum Key Distribution: A Networking Perspective," *ACM Computing Surveys*, vol. 53, no. 5, 2020, pp. 1–41.
[6] S.-K. Liao *et al.*, "Satellite-to-Ground Quantum Key Distribution," *Nature*, vol. 549, no. 7670, 2017, pp. 43–47.
[7] J. Yin *et al.*, "Entanglement-Based Secure Quantum Cryptography Over 1,120 Kilometres," *Nature*, vol. 582, no. 7813, 2020, pp. 501–05.
[8] H.-Y. Liu *et al.*, "Optical-Relayed Entanglement Distribution Using Drones as Mobile Nodes," *Physical Review Letters*, vol. 126, no. 2, 2021, p. 020503.
[9] Y. Wang *et al.*, "A Survey on Metaverse: Fundamentals, Security, and Privacy," arXiv preprint arXiv:2203.02662, 2022.
[10] Y. Cao *et al.*, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," *IEEE Commun. Surveys & Tutorials*, 2022.
[11] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, vol. 108, no. 13, 2012, p. 130503.
[12] Y. Zhao and C. Qiao, "Redundant Entanglement Provisioning and Selection for Throughput Maximization in Quantum Networks," *Proc. IEEE Conf. Computer Commun.*, IEEE, 2021, pp. 1–10.
[13] H.-Y. Liu *et al.*, "Drone-Based Entanglement Distribution Towards Mobile Quantum Networks," *National Science Review*, vol. 7, no. 5, 2020, pp. 921–28.
[14] M. Mehic *et al.*, "A Novel Approach to Quality-Ofservice Provisioning in Trusted Relay Quantum Key Distribution Networks," *IEEE/ACM Trans. Networking*, vol. 28, no. 1, 2019, pp. 168–81.
[15] Y. Cao *et al.*, "Hybrid Trusted/Untrusted Relay-Based Quantum Key Distribution Over Optical Backbone Networks," *IEEE JSAC*, vol. 39, no. 9, 2021, pp. 2701–18.

Biographies

Minrui Xu (minrui001@e.ntu.edu.sg) received the B.S. degree from Sun Yat-Sen University, Guangzhou, China, in 2021. He is currently working toward the Ph.D. degree in the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests mainly focus on trustworthy machine learning, deep reinforcement learning, and incentive mechanism design.

Dusit Niyato [M'09, SM'15, F'17] (dniyato@ntu.edu.sg) is currently a professor in the School of Computer Science and Engineering, Nanyang Technological University, Singapore. He received the B.Eng. degree from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand in 1999 and Ph.D. in electrical and computer engineering from the University of Manitoba, Canada in 2008. His research interests are in the areas of Internet of Things (IoT), machine learning, and incentive mechanism design.

Zehui Xiong [M'20] (zehui_xiong@sutd.edu.sg) is an Assistant Professor at Singapore University of Technology and Design. Prior to that, he was a researcher with Alibaba-NTU Joint Research Institute, Singapore. He received the Ph.D. degree in Computer Science and Engineering at Nanyang Technological University, Singapore. He was a visiting scholar with Princeton University and University of Waterloo. His research interests include wireless communications, network games and economics, blockchain, and edge intelligence.

Jiawen Kang (kavinkang@gdut.edu.cn) received the M.S. degree and the Ph.D. degree from the Guangdong University of Technology, China, in 2015 and 2018, respectively. He is currently a full professor at the Guangdong University of Technology. He was a postdoc at Nanyang Technological University from 2018 to 2021, Singapore. His research interests mainly focus on blockchain, security, and privacy protection in wireless communications and networking.

Xianbin Cao (xbcao@buaa.edu.cn) received the Ph.D. degree in signal and information processing from the University of Science and Technology of China, Hefei, China, in 1996. He is the Dean and a Professor with the School of Electronic and Information Engineering, Beihang University, Beijing, China. His research interests include intelligent transportation systems, airspace transportation management, and intelligent computation.

Xuemin (Sherman) Shen [M'97, SM'02, F'09] (sshen@uwaterloo.ca) is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on network resource management, wireless network security, AI for networks, 5G and beyond, and vehicular networks. He is a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Chinese Academy of Engineering Foreign Member. He received the R.A. Fessenden Award in 2019 from IEEE, Canada; the James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society; and the Joseph LoCicero Award in 2015 and Education Award in 2017 from the IEEE Communications Society.

Chunyan Miao (ascymiao@ntu.edu.sg) is currently a professor in the School of Computer Science and Engineering, Nanyang Technological University (NTU), and the director of the Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY).

We can observe that as the number of Metaverse applications increases, the provisioning costs of all three models increase accordingly. Moreover, the performance difference in provisioning cost among the three models is also larger as the number of Metaverse applications increases.